Anonymisierungsdienste im Internet

Von Cand. Wi-Ing. Bastian Schwark
Universität Karlsruhe (TH)

Im Gegensatz zur realen Welt, in der der Mensch die Wahl hat zwischen Anonymität und Darlegung seiner personenbezogenen Daten, hinterlässt der Nutzer bei jeglicher Kommunikation im Internet - ob gewollt oder ungewollt - eine Vielzahl von Informationen.

Bedingt durch dieses "Verdrehen der Vorzeichen" im Internet zeigen sich jedoch immer mehr Nutzer sensibilisiert und äußern Besorgnis bezüglich ihrer personenbezogenen Daten. Die Problematik elektronischer Kommunikation wird im wesentlichen durch zwei Gründe hervorgerufen. Zum einen fehlt das Wissen um den sicherheitstechnischen Standard der elektronischen Kommunikation ("environmental control"), so dass der Nutzer letztendlich die Bedingungen blind akzeptieren muss, zum anderen geht die Kontrolle über die übermittelten personenbezogenen Daten ("secondary use of information") verloren.[1]

Der Anreiz, sich personensensible Daten zu beschaffen, muss nicht immer ökonomischer Natur sein, denn auch Arbeitgeber, Versicherungen, Geheimdienste und Strafverfolgungsbehörden zählen zu den potentiellen Interessenten. Der Großteil der Aktiven stellen jedoch Firmen dar, die, abhängig von Quantität und Qualität der Kundendaten, profitabiliätssteigernde Service- und Produktdifferenzierungen im Sinne des Customer Relationship Management (CRM) betreiben wollen.

Da im Internet ein herkömmlicher Ausgleich von Vertrauensbildung und Transparenz nicht zu wirken scheint, verbleibt es also beim Nutzer sein Selbstbestimmungsrecht über seine personenbezogenen Informationen auch in diesem Medium auszuüben. Zur praktischen Durchführung stehen dem Nutzer eine Reihe etablierter Anonymisierungsdienste zur Verfügung, die jedoch unterschiedlichen sicherheitstechnischen Standards genügen. Der vorliegende Artikel soll dem Leser zum Verständnis und zur Differentiation der grundlegenden technischen Konzepte der etablierten Anonymisierungsdienste beitragen.

Spuren im Netz

Grundsätzlich hat jeder Betreiber von Infrastruktur für das Internet sowie diejenigen, die die Möglichkeit besitzen, darauf zuzugreifen, die Option zu beobachten und somit an personenbezogene Daten zu gelangen. Allen voran ist hier der Internet Service Provider (ISP) zu nennen, welcher durch die Speicherung von Nutzungsdaten zum Zwecke der Abrechnung auch die Zuordnung der dynamischen IP-Adressen während eines entsprechenden Zeitraums durchführen kann. Die IP-Adresse, momentan durch das Internet-Protokoll IPv4 auf eine 32 Bit lange Zahl festgelegt,[2] gilt als eindeutige Kennung für den Internetnutzer und somit als sensibles Datum.[3] Doch nicht nur ISP, sondern ebenso Betreiber von Router, Netzwerkadministratoren und andere Nutzer im gleichen Intranet haben die Möglichkeit zur Beobachtung. Externe Bobachter haben hingegen, sofern sie nicht durch den Beobachteten bzw. seinen Rechner unterstützt werden, erschwerten Zugang.[4]

Selbst bei vollständigem Vertrauen des Nutzers in die Sicherheit der Infrastruktur, haben die Anbieter von Websites im Internet Methoden entwickelt, welche die ohnehin beschränkte Anonymität durch die dynamischen IP-Adressen vollständig aushöhlen können. Bekannte Beispiele hierfür wären beispielsweise Cookies, Web-Bugs, HTTP-Header-Informationen und JavaScript, die jedoch hier nicht näher dargestellt werden können.

Begriffsbestimmungen

Um die "State of the Art" Umsetzungen von Anonymität im Internet durch so genannte "Anonymisierer" im Internet darzustellen, ist es zunächst notwendig, dass die folgende Begriffsbestimmung eine einheitliche Ausgangsbasis ermöglicht.

Wenn man von "Internet-Diensten" spricht, so sind hier die im Rahmen der Anonymisierung wichtigen Dienste HTTP, FTP, SMTP und NNTP. Dabei dient HTTP im Internet zur Übermittlung der Webseiten zwischen Client und Server; FTP hingegen dem effizienten Datenaustausch, wobei hier zwischen Kontrollnachrichten und den eigentlichen Daten unterschieden wird. SMTP dient zur Übermittlung elektronischer Post, welches wie HTTP hierfür eine bidirektionale Verbindung zwischen Client und Server aufbaut. Als Letztes wäre NNTP zu nennen, welches zum Abfragen, Posten und Verteilen von News Artikeln dient.

Der wesentliche Unterschied zwischen den oben genannten Diensten ist, dass es sich bei E-Mail und News (SMTP und NNTP) um asynchrone Dienste handelt und somit die Nachricht nicht sofort beim Empfänger ankommen muss. Deshalb können reine E-Mail-Anonymisierungsdienste auf anderen technischen Realisierungen beruhen und werden getrennt von Web und FTP behandelt.[5]

[1] Culnan, M. J., "Consumer Awareness of Name Removel Prodcedures: Implications for Direct Marekting", vol. 9, 1995/2, S. 10-19.

[2] Das künftige Internet-Protokoll IPv6 sieht eine IP-Adresse von 128 Bit vor, wodurch sich 10^{29} mal so viele verschiedene Adressen vergeben lassen. Die Problematik der Anonymität wird sich also noch zusätzlich verschärfen, da jedem Menschen dann 10^{32} IP-Adressen zugewiesen werden können. Momentan ist die Mächtigkeit des Zahlenraumes zu gering für die Menge der Internetnutzer, so dass diese dynamisch vergeben werden. Die IP-Adresse kann sich auch während einer Sitzung ändern.

[3] Köhntopp, Marit, Köhntopp, Christian: Datenspuren im Internet, Computer und Recht (CR) Nr. 4, 2002; S. 248.

[4] Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein (Hrsg.), Sicherheit im Internet durch Anonymität, August 2002, Seite 8-9.

Eine weitere Definition ist für die Unterscheidung zwischen Client- und Server-Anonymität notwendig. Von **Client-Anonymität** wird gesprochen, wenn ein Nutzer eines Dienstes seine Identität nicht preisgeben möchte, während **Server-Anonymität** die Anonymität des Diensteanbieters gewährleistet. Wesentliches Hindernis hierbei ist, dass die URL-Adresse (Universal Ressource Locator) des Benutzers bekannt sein muss.[6]

Abschließend soll an dieser Stelle noch auf den eigentlichen Begriff der **Anonymisierung** eingegangen werden. "Anonymisierung ist eine Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Dies ist eine strengere Definition, wie sie beispielsweise in § 2 Abs.2 Nr.7 LDSG SH (Landesdatenschutz-Gesetz Schleswig-Holstein) verwendet wird. Das Bundesdatenschutzgesetz (§ 3 Abs.7 BDSG) und andere Landesgesetzte (wie z.B. Art. 4 Abs.8 BayDSG) ersetzen allerdings die strenge Anforderung "*nicht mehr*" durch "*nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft*".

Unbeobachtbarkeit ist sogar noch eine stärke Forderung als Anonymität, denn unbeobachtbar ist ein Nutzer erst dann, wenn beliebige Beobachter nicht einmal feststellen können, ob dieser überhaupt kommuniziert. Dies lässt sich nur mit einem hohen Prozentsatz an leerem Datenverkehr (Dummy-Traffic) umsetzen, scheitert aber in der Regel an der Realisierung, da durch das hohe Verkehrsaufkommen zusätzliche Kosten und Performanceeinbußen entstehen.[7]

Eine **Pseudonymisierung** hingegen bedeutet das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können. Aufgrund der Tatsache, dass ein solches Verfahren immer auch den Personenbezug unter entsprechenden Rahmenbedingungen wiederherstellen soll, sollte es auch nur dort eingesetzt werden, wo Anonymisierung nicht möglich ist.[8]

Grundsätzlich tritt bei der Pseudoanonymisierung die Problematik auf, dass bei einem Pseudonymisierer Name und Pseudonym zusammenlaufen. Solche Dienste gewährleisten also mitnichten eine vollständige Anonymität. Der Vorteil bei einem Pseudonymisier-Remailer, d.h. die Verwendung von Pseudonymen bei einem E-Mail Dienst, liegt auf der Hand, denn die anonymen Absender sind unter ihrem Alias für Antworten erreichbar. Solche Dienste könnten letztendlich aber ein ähnliches Schicksal erleiden wie der finnische Pseudonymisier-Remailer -"anon.penet.fi". Nach einer Polizeiaktion wurde bei "Penet" jedoch mit einem Schlag auch die Anonymität der anderen 700.000 Penet-User aufgehoben. Der Betreiber sah sich danach außer Stande, den Dienst weiter zu betreiben.

PGP

PGP steht für Pretty Good Privacy und stellt eine Realisierung einer asymmetrischen bzw. hybriden Kryptoverschlüsselung dar. Hierfür existieren zwei Schlüssel, ein öffentlicher und ein privater, wobei der Sender lediglich über den öffentlichen Schlüssel verfügt. Der davon unterschiedliche private Schlüssel besitzt jedoch lediglich nur der Empfänger. Weiter Informationen sowie neueste Version sind unter http://www.pgpi.org downloadbar. Es gibt noch weitere hybride Kryptosysteme wie beispielsweise TLS - Transport Layer Security.

▲ ***Kasten 1***

E-Mail und News Anonymisierungsdienste

Typ 1-Remailer (Cypherpunk-Remailer

Der erste Typus von anonymer und unbeobachteter E-Mail stellt der Cypherpunk-Remailer dar, wobei ein Remailer einen speziellen Server darstellt, über den der Mailverkehr läuft. Jeder dieser so genannten Typ 1-Remailer verfügt über eigene öffentliche Schlüssel einer hypriden Kryptoverschlüsselung (PGP - siehe Kasten 1).

Der Absender verschlüsselt also die gesamte Nachricht einschließlich der Empfängeradresse mit dem öffentlichen Schlüssel des Remailers und sendet das Chiffrat an diesen. Der Remailer (und nur dieser) kann die Nachricht mit seinem privaten Schlüssel entschlüsseln, liest dabei die Empfängeradresse aus, sendet die Nachricht an den Empfänger weiter und unterdrückt die Adresse des wahren Absenders.

Weitaus sicherer wird diese Methode, wenn die E-Mail eine verschachtelte Kette von Cypherpunk-Remailern durchläuft, wobei nur der letzte Remailer die eigentliche Empfängeradresse kennt. Die Nachricht muss also hierzu mehrmals chiffriert werden, beginnend mit dem öffentlichen Schlüssel des letzten Remailers. Sofern nur einer dieser Remailer vertrauenswürdig ist, ist die Anonymität gewährleistet. Diese angesprochene Kaskadierung (Hintereinanderschaltung) ähnelt schon stark dem Mix-Modell von Chaum (siehe Kasten 2). Durch Vorgabe einer zufälligen Zeitspanne an die Remailer, nach der sie erst die E-Mail weiterleiten dürfen, lässt sich das Nachvollziehen des Weges durch das Internet zusätzlich erschweren.[9]

Weiterhin kann dieser Typ 1-Remailer auch zum anonymen Empfang von E-Mails verwendet werden. Hierzu wird die "Rückadresse" des Mix-Modells benötigt. Der Nutzer benötigt dazu eine Art anonyme leere Nachricht an sich selbst um so einen Reply-Block aufzubauen. Als weitere Information enthält die Nachricht jedoch für jeden einzelnen Remailer einen individuellen symmetrischen Schlüssel (beide Parteien besit-

[6] Eckert Claudia, Pircher, Alexander, Anonym im Internet, in Horster, Patrick (Hrsg.): Kommunikationssicherheit im Zeichen des Internet, Braunschweig/Wiesbaden, 2001, Seite 15-18.

[6] Demuth, Thomas, Rieke, Andreas: Anonym im World Wide Web?, DuD, 1998/11, Seite 623-624.

[7] Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein (Hrsg.), Sicherheit im Internet durch Anonymität, 2002, Seite 14.

[8] Arbeitskreis Technik der Datenschutzbeauftragten, Datenschutzfreundliche Technologien, DuD, 1997/12, Seite 710-711.

[9] c't 16/2002, Anonymität: Remailer, S.156, abrufbar unter <http://www.heise.de/ct/00/16/156/>. Rev. 2004-09-18.

zen den gleichen Schlüssel). Sendet nun ein Dritter eine Nachricht unter Verwendung dieses Reply-Blocks, verschlüsselt jeder Remailer die Nutzlast mit seinen symmetrischen Schlüssel.

Zu den wirksamen Angriffen, die gegen solche Anonymisierungsdienste durchgeführt werden können, gehört die Überwachung der Nachrichten vor und nach jedem Knoten. Da sich hier die Nachricht verkürzt, kann sie somit verfolgbar werden. Ebenso kann bei so einer "totalen Überwachung" eine Korrelation zwischen den Zeitpunkten hergestellt werden, in welchem die Nachricht vom Absender an den Empfänger gelangt. Somit kennt der Angreifer die Kommunikationsbeziehung zwischen beiden. Kritisch wird es jedoch besonders, wenn durch "Replay-Angriffe" versucht wird, die bestehende Kommunikationsbeziehung aufzudecken. Der Angreifer sendet in diesem Falle eine legitime, aufgefangene Nachricht mehrmals an den Remailer und gewinnt dadurch in jedem Falle Rückschlüsse. Eine Vermeidung auf Rückschlüsse durch den Zeitpunkt könnte verhindert werden, indem jeder Beteiligte selbst einen Remailer betreibt, und somit der Mail-Verkehr nicht mehr zuzuordnen ist.[10]

Typ 2-Remailer (Mixmaster-Remailer

Eine Fortentwicklung der oben genannten Remailer stellt das 1995 vorgestellt Mixmaster-Verfahren von Cottrel dar, welches die Schwächen des bis dato nur verfügbaren Typ 1-Remailers aufhob.[11] Das Mixmaster-Verfahren basiert auf dem Mix-Modell (siehe Kasten 2). Zwar bleibt das Versenden von Dummy-Traffic aus, dafür agiert aber der Mixmaster mit einem zusätzlichen Sicherheitsprinzip. Die Nachrichten, die in einem Schub einen Mix erreichen, werden nicht alle umkodiert und weitergesendet, sondern immer eine konstante Menge von Nachrichten vorgehalten. Der Angreifer verliert somit jeglichen Anhaltspunkt, zu welchem Zeitpunkt die Nachricht den Mix verlassen haben könnte.[12]

Um Nachrichten nicht anhand der Länge identifizieren zu können, haben alle Nachrichten im Mixmaster-System eine fixe Länge von ca. 28 kB, was durch Abspalten oder Auffüllen mit zufälligem Material erreicht wird. Das Prüfen auf Duplikate wird mit Hilfe einer Message-ID erreicht und diese Duplikate zur Vermeidung von Replay-Angriffen vernichtet. Der bei Typ 1 vorgestellte Weg, über Reply-Blöcke Antworten zu bekommen, ist in Mixmaster allerdings nicht vorgesehen. Empfängeranonymität ist hier

[10] Roessler, Thomas, Anonymität im Internet, DuD, 1998/11, S. 620.

[11] BSI, Bundesamt für Sicherheit in der Informationstechnik, Das Ende der Anonymität?, Kapitel 6.1, abrufbar unter <http://www.bsi.bund.de/literat/anonym/index.htm>. Rev. 2004-09-18.

[12] Kesdogan, Dogan, Privacy im Internet - Vertrauenswürdige Kommunikation in offenen Umgebungen, Braunschweig/Wiesbaden, 2000, S. 76.

▼ ***Kasten 2***

Das Mix-Modell

Der Grundlagenaufsatz der umkodierenden Mixe zur Anonymität und Unbeobachtbarkeit in Vermittlungsnetzen wurde 1981 von David Chaum veröffentlicht.[13] Das Mix-Modell gilt heute, sowohl beim Einsatz für E-Mail als auch als Web-Anonymisierung, als eines der wenigen Gewährleistungen einer "starken" Anonymität, d.h. dass die Anonymität nicht nur von einem einzigen vertrauenswürdigen Dritten abhängt.

Nach Chaum sendet ein Sender seine Nachricht nicht direkt an den Empfänger, sondern über mehrere hintereinander geschaltete Rechner, die so genannten Mixe. Um Angreifern keine Möglichkeit der Verkettbarkeit zu geben, halten diese Mixe die eingehenden Nachrichten solange gespeichert, bis eine bestimmte Anzahl von Nachrichten erreicht ist. Die Mixe sortieren einerseits die Reihenfolge der Nachrichten neu und kodieren sie zusätzlich um. Um eine Verkettung zwischen eingehender und ausgehender Nachricht zu vermeiden, haben alle Nachrichten die gleiche Länge. Eine mögliche Angriffsform gegen so ein System wäre das Abfangen einer regulären gesendeten Nachricht und das Weitersenden einer Vielzahl der gleichen Nachricht. Dies ist insofern problematisch, als dass das Umkodieren deterministisch erfolgt, d.h. dass der Mix unter gleichen Voraussetzungen immer wieder gleich umkodiert und es somit relativ einfach möglich wäre, einzelne Mixe zu überbrücken. Um so einer Angriffsmöglichkeit entgegenzuwirken, werden Nachrichten geprüft, ob sie bereits gemixt worden sind. Zwei Gefahren lauern allerdings trotzdem in diesem Prinzip. Da nämlich eine Nachricht nur innerhalb eines Schubes anonym ist, darf der Angreifer nie alle Nachrichten außer einer Einzigen selbst erzeugt haben, da diese folglich enttarnt wäre (n-1 Angriff). Ähnliches Resultat würde sich ergeben, falls alle Sender und Empfänger bis auf Einen in einem Schub zusammen arbeiten würden.

Zusätzlich müssten alle Sender zu jedem Zeitpunkt genau eine Nachricht senden und auch alle Empfänger eine Nachricht empfangen, da sich sonst die zu beobachtenden Anzahl der Teilnehmer verringert und eine Zuordnung von Sender und Empfänger einer Nachricht unter Umständen möglich wäre. Diejenigen Teilnehmer, die nichts zu senden haben, senden Dummy Traffic, d.h. Leernachrichten, um die Sender- und Empfängergruppe konstant zu halten.[14]

Das Herzstück des Umkodierens sei an Abbildung 1 erklärt. Jeder Mix entschlüsselt die Nachricht mit seinem privaten Schlüssel eines asymmetrischen bzw. hybriden Kryptosystems (PGP), kodiert sie um und verschickt sie weiter, wobei nur der letzte Remailer in der Kaskade die eigentliche Zieladresse entschlüsseln kann. Die Chiffrierung erfolgt somit mit dem öffentlichen Schlüssel des nächstliegenden Mix, wobei nur dieser über den privaten Schlüssel zum Dechiffrieren verfügt.

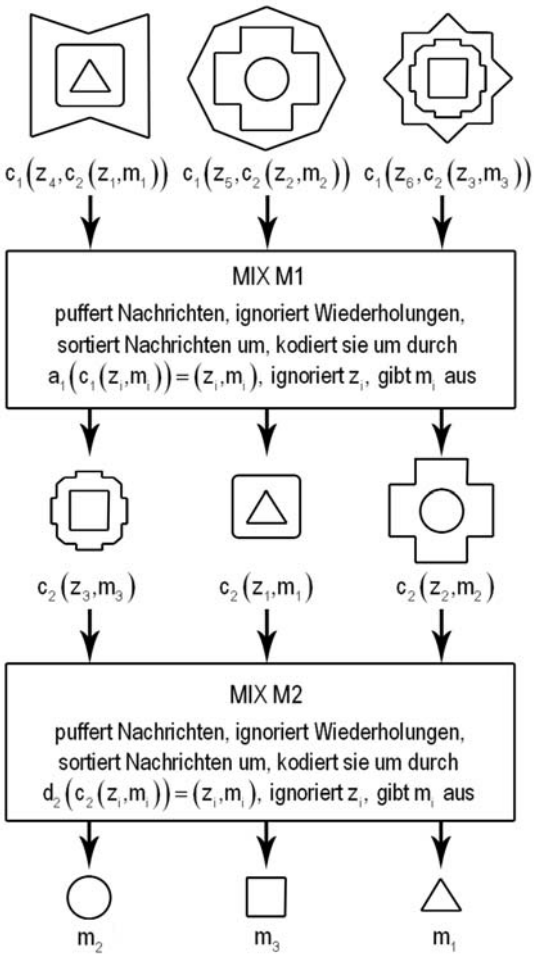
Jeder Mix kennt folglich nur seinen Vorgänger und Nachfolger, wobei der Erste den Absender kennt und der Letzte den angefragten Web-Server. Sicherheit in Bezug auf Anonymität ist bei diesem Modell dann gewährleistet, sobald mindestens ein Mix vertrauenswürdig ist.

[13] Chaum, D. Ultraceable Electronic Mail, Return Adresses and Digital Pseudonyms, Communications of the ACM, Vol. 24, 1981, S. 84-88.

[14] Federrath, Hannes, Umkodierende Mixe, DuD, 2003/3, S. 169.

also nur über Newsgroups wie Usenet möglich.[15]

Geeignete Programme, die sowohl mit Cypherpunk- als auch mit Mixmaster-Remailern umgehen können, sind "Private Idaho"[16] und "Jack B. Nymble"[17]. Ein reiner Mixmaster E-Mail-Client ist das übersichtliche Programm "Quicksilver"[19], welches die verfügbaren Remailer automatisch checkt und die Verschlüsselung übernimmt.



▲ Abbildung 1: Umkodieren zu mixender Nachrichten (Zeichenerklärung: m: Nachricht; z: zufällige Zeichenkette; c: öffentlicher Schlüssel; d: privater Schlüssel)[18]

Mit beiden vorgestellten E-Mail Anonymisierungsdiensten kann auch eine Empfängeranonymität realisiert werden. Die Nachricht wird hierzu anonym und mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und in einer so genannten Usenet-Gruppe veröffentlicht. Der Empfänger lädt von Zeit zu Zeit alle Nachrichten aus der Usenet-Gruppe auf seinen Computer und versucht, die Nachrichten zu dechiffrieren. Der Empfänger kann jedoch nur diejenige im Klartext lesen, die für ihn bestimmt sind.[20] Da mit der gleichen Technik E-Mails und News abgewickelt werden kann, wurde nur von zu anonymisierenden E-Mails gesprochen.

WWW und FTP Anonymisierungsdienste

Der einfachste Typus eines Web-Anonymisierungsdienstes, welcher die Server-Log-Datei anonymisiert, sei hier nur beiläufig erwähnt. In der Server-Log-Datei werden die Zugriffe auf das Internet protokolliert, und beim Einbau eines solchen Dienstes in den Browser können die Daten bereits anonymisiert in die Log-Datei eingetragen werden. Der Nutzer hat hierbei allerdings keine Kontrollmöglichkeit. Da existierende Verfahren eine Anonymisierung nur sehr lückenhaft durchführen, eignen sich diese nicht für eine sichere Anwendung. So wird beispielsweise das Referer-Feld im HTTP-Header, in welchem die zuvor besuchte Webeseite eingetragen ist, unverschleiert in der Log-Datei des Servers protokolliert.[21]

Proxies

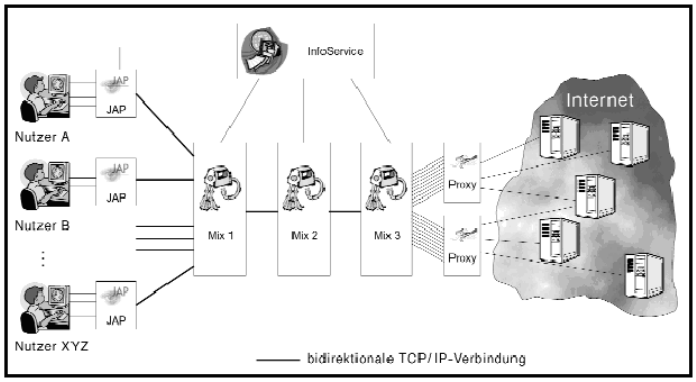
Die bekannteste Klasse der Anonymisierungsdienste sind wohl die der anonymisierenden Proxies ("Stellvertreter"). Weltweite bekannte Dienste sind sowohl der "Anonymizer"[22] als auch der Lucent Personalized Web Assistant[23]. Der Name Proxy ("Stellvertreter") rührt daher, dass eine dritte Partei zwischengeschaltet ist und Proxy-Systeme oft über einen Cache (Speicher) für Internet-Seiten verfügen, um bereits aufgerufene Seiten schneller lokal verfügbar zu machen. Somit tauchen in den Logfiles der Webseite, in denen sonst personenbezogene Daten gespeichert werden könnten, lediglich die Informationen des Betreibers des Anonymisierungsdienstes auf. So erscheint zum Beispiel ausschließlich die IP-Adresse des Dienstes beim Webserver. Falls der Cache nicht beim Betreiber eines solchen Dienstes liegt, können unter anderem über "Anonymity4Proxy"[24] Millionen anderer, so genannter offener Proxies, im Internet nach der gesuchten Internet-Seite abgesucht werden, streng darauf basierend, dass die angefragten Proxies keine Daten aufzeichnen.

Der Nutzer ruft hierzu die Webseite des Anonymisierdienstes auf und gibt in einem Web-Formular die URL der gewünschten Webseite ein. Der Anonymisierdienst erhält hiermit die Rolle eines Mittelsmanns und untersucht die Anfrage auf verräterische Informationen im HTTP-Header. Ebenso werden die vom Web-Server gesendeten Antworten beispielsweise von aktiven Inhalten und Cookies gefiltert. Links, die in der angefragten Seite enthalten sind, werden so geändert, dass sie bei Aufruf auch wieder über den Proxy verlaufen würden. Die oben genannten Dienste unterstützen auch den anonymen Versand von E-Mails.

Der Nachteil des Einsatzes eines einfachen Proxy-Dienstes ist der, dass der Proxy das Surfverhalten der Nutzer beobachten kann und ihm so in Bezug auf das Sammeln von Verkehrsinformationen und Interessensdaten vertrauen muss. Der Nutzer hätte jedoch die Möglichkeit, selbstständig mehrere solcher Proxy-Dienste hintereinander zu schalten, wobei dann nur der erste Proxy wirklich weiß, welche IP-Adresse den

[15] Roessler, Thomas, Anonymität im Internet, S. 620.
[16] http://www.fluidlight.com/privateidaho/.
[17] http://www.skuz.net/potatoware/ (Die Weiterentwicklung wurde allerdings eingestellt.).
[18] Federrath, Hannes, Pfitzmann, Andreas: "Neue" Anonymitätstechniken, DuD, 1998/11, S. 629.
[19] http://quicksilver.skuz.net/.
[20] Roessler, Thomas, Anonymität im Internet, S. 620.
[21] Eckert Claudia, Pircher, Alexander: Anonym im Internet, Seite 20.
[22] http://www.anonymizer.com.
[23] LPWA, http://www.bell-labs.com/project/lpwa/overview.html.
[24] http://www.inetprivacy.com/a4proxy/index.htm.

Dienst nutzt. Eine Verschlüsselung wird hier im Regelfall nicht verwendet, so dass Angreifer sämtliche Inhalte mitlesen könnte, es sei denn, dass die Anonymisierdienste Verschlüsselungen wie SSL (Secure Socket Layer) unterstützen und der Nutzer somit eine sichere Verbindung zum Proxy herstellt. Die Datenübertragung von Proxy zu Server bleibt jedoch trotzdem unverschlüsselt. Hinsichtlich Verkehrsanalysen ist die Kommunikation solcher Dienste generell nicht sicher, da eine Korrelation sowohl von Zeit als auch Länge ein- und ausgehender Nachrichten besteht.



▲ ***Abbildung 2: Architektur des Anonymisierungsdienstes JAP[28]***

Weitere Dienste, welche Anfragen über offene Proxies umleiten, sind zum Beispiel "Steganos Internet Anonymität"[25] und erschweren somit eine Rückverfolgung der Kommunikation. Die Proxies werden teilweise jede Minute gewechselt; ein einzelner Proxy hat deshalb nur beschränkten Überblick.[26] Auch beim "Rewebber"-Dienst (ehemals Janus und damals Forschungsprojekt der Fern-Universität Hagen) wird die Client-Anonymität über Proxies hergestellt, allerdings mit der Besonderheit, dass der "Rewebber" zusätzlich als einziger Dienst auch das anonyme Publizieren realisierte. Aufgrund mangelnder Nachfrage musste dies jedoch wieder eingestellt werden.

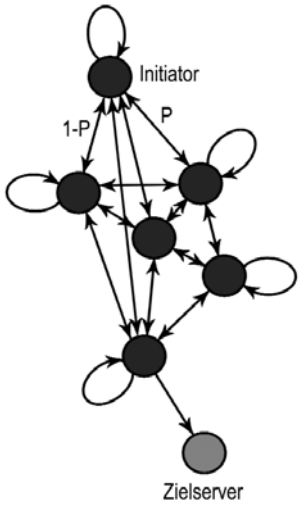
Mixe

Einen weiteren Schritt in Richtung Sicherheit geben die Mix-basierten Web-Anonymisierungsdienste vor. Ein älterer, bekannter Dienst war Onion-Routing, dessen Testbetrieb allerdings seit Januar 2000 eingestellt worden ist.[27] Er arbeitete als Proxy-Dienst mit einem Initiator-Proxy auf der Client Seite und einen Responder-Proxy auf der Server-Seite. Dazwischen waren mehrere Onion-Router nach dem Mix-Modell geschaltet.

Ein ähnliches Prinzip verfolgt auch das Forschungs- und Entwicklungsprojekt "AN.ON - Starke Anonymität im Internet", welches seit September 2000 der Öffentlichkeit zur Verfügung steht und vom Bundeswirtschaftsministerium gefördert wird.[29] Das Anonymisierungssystem besteht aus einer Client-Software mit dem Namen JAP, mehreren Anonymisierungsstationen (den Mixen) und einem InfoService. Abbildung 2 veranschaulicht diesen Sachverhalt graphisch. Die Proxy-Schnittstellen sind wie bei Onion-Routing angeordnet.

Zum Benutzen von AN.ON muss der Web-Surfer die Software JAP auf seinem Rechner installieren und steht so zwischen Browser und Internet. Wird nun eine URL in JAP eingegeben, wird sie nach dem bekannten Prinzip mehrmals für die zu durchlaufende Mix-Kette verschlüsselt. Die aus der Anfrage entstehende "Zwiebel" wird nun zum ersten Mix gesendet, welcher die erste Verschlüsselungsschicht entfernt. Die Schlüsselinformationen und Verbindungsdaten werden nun in eine Tabelle eingetragen und die "gepellte Zwiebel" weitergeleitet, bis die Verbindung zum eigentlichen Ziel aufgebaut ist. Da eine HTTP-Anfrage bidirektional erfolgt, wird die bestehende Verbindung zur bidirektionalen Übertragung von Nutdaten genutzt, d.h. dass alle Daten den gleichen Weg durch die Mixe nehmen. So erhält der Nutzer auf demselben Weg zurück schließlich seine Daten, so dass ein beliebiger zwischengeschalteter Mix ausschließlich Vorgänger und Nachfolger kennt.[30]

Weiterhin kommt in JAP ein erweitertes Mix-Konzept zur Anwendung. Mehrere Mix-Pakete werden bei der Übertragung zu einem Mixkanal zusammengefasst, welche über die Kanal-ID gesteuert wird. Diese ist jeweils nur zwischen zwei Mixen bzw. Client und Mix gültig, da sonst bei gleicher ID dazwischen liegende Mixe überbrückt werden könnten. Mittels eines zeitlichen "Verfallsdatums" einer Nachricht, speichert ein Mix diese und überprüft sie auf Nachrichtenwiederholung, um "Replay"-Angriffe abzuwehren. Auch haben die Nachrichten alle dieselbe Länge. Die Gefahr eines (n-1) Angriffes bleibt aber auch bei AN.ON nach wie vor bestehen. Die verfügbaren, fest definierten Mix-Kaskaden, sind über den InfoService



▲ ***Abbildung 3: Funktionsprinzip eines Peer-to-Peer Dienstes[31]***

[25] http://www.steganos.de.

[26] Köpsell, Stefan, Federrath, Hannes, Hansen, Marit: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, DuD, 2003/3, S. 139.

[27] http://www.onion-router.net.

[28] Köpsell, Stefan, Federrath, Hannes, Hansen, Marit, Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, S. 140.

[29] AN.ON steht für Anonymity Online und ist ein Gemeinschaftsprojekt des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, der Technischen Universität Dresden und der Freien Universität Berlin, http://anon.inf.tu-dresden.de/.

[30] Roessler, Thomas: Anonymität im Internet, S. 621

[31] Langheinrich, Moschgath, Vogt: Privacy im Zeitalter von Ubiquitous Computing, Folie 22, abrufbar unter <http://www.inf.ethz.ch/vs/edu/WS0001/UI/slides/ui_01privacy.pdf>. Rev. 2004-09-18.

ersichtlich, wovon der Nutzer eine auswählt.

Will der Nutzer zusätzlich erreichen, dass der letzte Mix der Inhalt der Seite verborgen bleibt, kann dies durch Verwendung von SSL erreicht werden. Der Webserver muss dies jedoch unterstützen. So erfährt der letzte Mix lediglich den Webserver, aber nicht die Seite, zu der er sich verbinden soll. Dies ist vorteilhaft für personalisierte Diensten im Internet wie Home-Banking, da hier die Benutzerdaten dem letzten Mix verborgen bleiben. Das System garantiert somit, dass zwar Client und Server bekannt miteinander kommunizieren können, aber gegenüber allen Außenstehenden, inklusive dem letzten Mix, anonym bleiben. Wird bei einem personalisierten Web-Dienst kein SSL (https) benutzt, so erfährt der letzte Mix den Benutzernamen. AN.ON realisiert hier eine Unverkettbarkeit von Identität und Benutzernamen, d.h. Pseudonymität.[32]

Vollständige Unbeobachtbarkeit konnte bei AN.ON jedoch aufgrund des fehlenden Dummy Traffics nicht realisiert werden. Zum einen scheitert dies an den schnellen Netzanbindungen der Nutzer, andererseits würde das Datenvolumen derart anwachsen, dass von allen Teilnehmern benutzerunfreundliche Verzögerungen hingenommen werden müssten.

Peer-to-Peer

Ebenso starke Entwicklungen gibt es derzeit auf dem Gebiet der der Peer-to-Peer basierten Systeme. Das bekannteste und wohl älteste ist "Crowds"[33], welches die Webanfragen in denen der anderen Teilnehmer versteckt. Der Nutzer meldet sich hierfür bei einer zentralen Stelle, dem Blender, an und installiert ein Programm. Im Falle von "Crowds" heißt dieses Programm Jondo und sorgt dafür, dass die Web-Anfrage nicht direkt an den Server weitergeleitet wird, sondern an einen anderen Jondo eines anderen Nutzer. In jedem wird zufällig entschieden, ob noch andere durchlaufen werden, oder die Anfrage direkt an den Server weitergeleitet wird (s. Abbildung 3). Neuere Peer-to-Peer Dienste sind Tarzan[34] und GNUnet.[35] Die Inhaltsdaten zwischen den Jondos sind mit einem symmetrischen Kryptosystem verschlüsselt. Verkettungen über die Länge der Nachrichten und der Zeit sind jedoch gegenüber Angreifern möglich.[36] Ein weiteres Problem stellen die möglicherweise langen Wartezeiten durch langsame Zugangsverbindungen einzelner Mitglieder dar.

Unfreiwillige Dienste

Keinen eigentlichen Dienst, aber dennoch eine Möglichkeit, sich anonym im Internet zu bewegen, stellen frei erhältliche Probezugänge von Internet-Service-Providern dar, die oft sogar frei Haus geliefert werden. Der zeitlich beschränkte ohne wirkliche Identitätsprüfung führt dazu, dass Aktivitäten im Internet fast nicht mit der realen Person des Nutzers in Verbindung gebracht werden können. Zusätzlich erschweren kann man so einen "Dienst", in dem man die Zugänge schachtelt oder häufig wechselt. Da allerdings, ebenso wie beim Gebrauch fremder Netzzugänge und der Übernahme von Netzknoten, der legale Weg verlassen wird, soll dies hier nicht weiter ausgeführt werden.[37]

Zusammenfassung

Neben den Peer-to-Peer basierten Anonymisierungssystemen, die aber gewisse rechtliche Problematiken aufzeigen, leistet allein das Mix-Modell im Web-Bereich bzw. dem Mixmaster-System bei E-Mails eine redundante Anonymität. Hier werden selbst bei Überwachung der gesamten Infrastruktur keine aufschlussreichen Rückschlüsse bekannt gegeben. Wer dennoch auf Nummer sicher gehen möchte, kann neben dem JAP noch Filterproxies den Feinschliff übernehmen lassen. ■

[32] Federrath, Hannes, Das AN.ON-System - Starke Anonymität und Unbeobachtbarkeit im Internet, in: Bäumler, Helmut, Mutius, Albert von (Hrsg.): Anonymität im Internet, Braunschweig/Wiesbaden, 2003, S. 176.

[33] Reiter, M. K., Rubin, A. D., Crowds: Anonymity for web transactions, ACM Transactions on Informations on Information and System Security, 1998, S. 66-92.

[36] http://www.pdos.lcs.mit.edu/tarzan/

[37] http://www.gnu.org/software/GNUnet.

[38] Federrath, Hannes, Pfitzmann, Andreas, "Neue" Anonymitätstechniken, S. 630.

[39] Roessler, Thomas, Anonymität im Internet, S. 621-622.

Karlsruher Transfer

Chefredaktion Bastian Schwark (V.i.S.d.P.)

Layout Christian Bock
Christian Bürger
Bastian Schwark
Martin Wagener

Redaktion Christian Bock
Martin Wagener
Florentine von Brunn

Herausgeber Verein Karlsruher Wirtschaftswissenschaftler e.V.

Druck Idee, Satz & Druck
Scheffelstr. 52
76135 Karlsruhe

Auflage 2500 Exemplare

Bezug Der Karlsruher Transfer erscheint einmal pro Semester. Er kann kostenlos von Interessenten bezogen werden.
ISSN 0937-0803

Anschrift Karlsruher Transfer
Verein Karlsruher Wirtschaftswissenschaftler e.V.
Waldhornstraße 27
76131 Karlsruhe
Tel.: 0721/608-3078
Fax: 0721/379824
transfer@vkw.org
www.vkw.org/transfer
wap.vkw.org